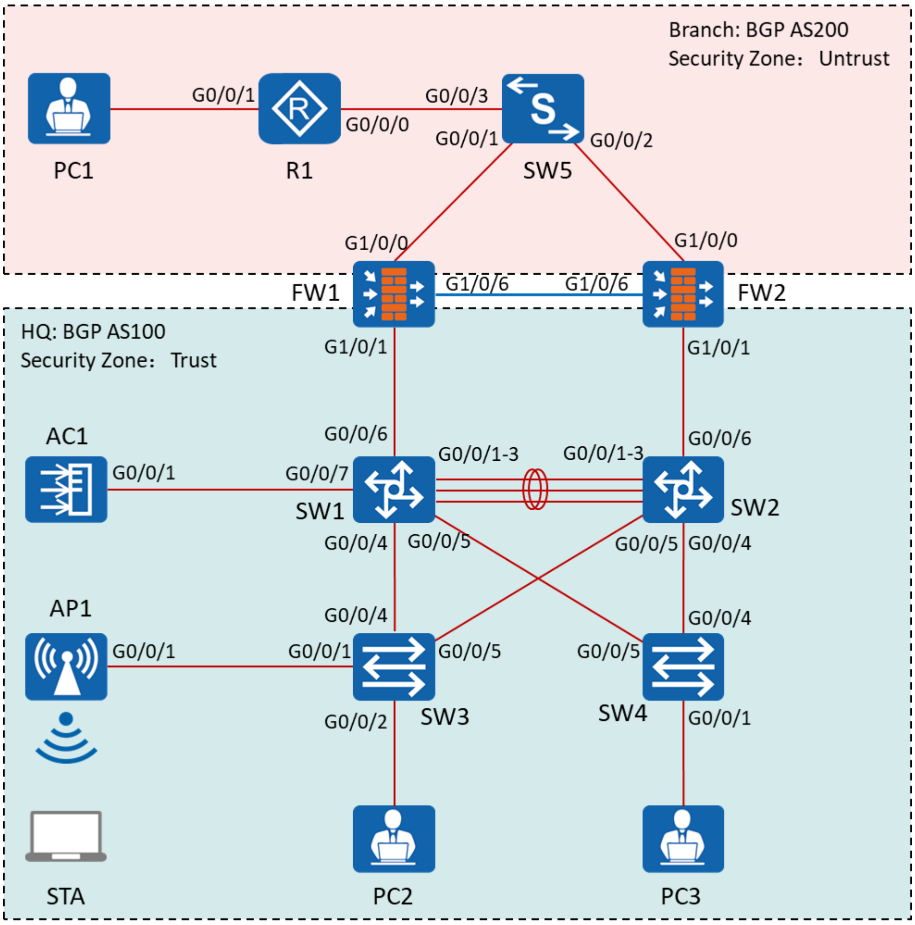
Huawei ICT Skill Competition Regional Mock Exam A (eNSP)

1 Background

This experiment simulates the interconnection between a large and medium-sized company headquarters and branches. In order to ensure the security of the campus network and the demands of internal staff for wireless office, firewalls and WLANs need to be deployed at the company headquarters.

2 Integrated network topology



Picture 2-1 Experimental topology

3 VLAN & IP address planning table

Table 3-1 VLAN planning table

Device name	Interface name	Port link type	PVID	Allow-pass VLAN
SW1	Eth-Trunk1(G0/0/1-G0/0/3)	Trunk	1	20 30
		Trunk	1	20 30
		Trunk	1	20 30
	G0/0/4	Trunk	1	15 20
	G0/0/5	Trunk	1	30
	G0/0/6	Access	10	10
	G0/0/7	Trunk	1	20 50
SW2	Eth-Trunk1(G0/0/1-G0/0/3)	Trunk	1	20 30
	G0/0/4	Trunk	1	30
	G0/0/5	Trunk	1	20
	G0/0/6	Access	10	10
SW3	G0/0/1	Trunk	15	15
	G0/0/2	Access	20	20
	G0/0/4	Trunk	1	15 20
	G0/0/5	Trunk	1	20
SW4	G0/0/1	Access	30	30
	G0/0/4	Trunk	1	30
	G0/0/5	Trunk	1	30
AC	G0/0/1	Trunk	1	20 50

Table 3-2 IP address planning table

Device name	Interface name	IP address
R1	Loopback 0	7.7.7.7/32
	G0/0/0	10.1.127.7/24
	G0/0/1	10.1.70.7/24
SW1	VLANif 10	10.1.13.3/24
	VLANif 15	10.1.15.1/24
	VLANif 20	10.1.20.13/24
	VLANif 30	10.1.30.13/24
	VLANif 50	10.1.50.1/24
	Loopback 0	3.3.3.3/32
SW2	VLANif 10	10.1.24.4/24
	VLANif 20	10.1.20.14/24
	VLANif 30	10.1.30.14/24
	Loopback 0	4.4.4.4/32
SW3	VLANif15	10.1.15.2/24
AC1	VLANif 50	10.1.50.2/24
	Loopback 0	8.8.8.8/32
FW1	G1/0/0	10.1.127.1/24
	G1/0/1	10.1.13.1/24
	G1/0/6	10.1.12.1/24
	Loopback 0	1.1.1.1/32
FW2	G1/0/0	10.1.127.2/24
	G1/0/1	10.1.24.2/24
	G1/0/6	10.1.12.2/24
	Loopback 0	2.2.2.2/32
PC1	/	10.1.70.1/24

Table 3-3 Device login information table

Device name	Management address	User	Password
Firewall	192.168.0.1:8443	admin	Huawei@123

Note: Please follow the instruction to configure the device name, policy ID, pool name, etc. Do not make the other naming by yourself. Otherwise you will get no point at that configuration.

3.1 VLAN

Configure VLAN information according to the contents of the VLAN planning table. The link type of the interconnect interface of SW1, SW2, SW3, SW4, and AC1 is configured as a trunk. The trunk link of the interconnect switches only releases the corresponding VLAN.

3.2 IP Address

Please follow the address information given in the exam planning topology and IP address planning table to connect and configure the IP addresses of the corresponding network devices and interfaces.

3.3 Link Aggregation

In order to ensure the link reliability between SW1 and SW2, SW1 and SW2 are connected to each other through G0/0/1, G0/0/2, and G0/0/3 interfaces, and these three interfaces are bundled into one logical interface (Eth-Trunk 1). SW1 is the active end (priority is 100), and the G0/0/1-2 interfaces are the active links (priority is 100).

3.4 MSTP

To prevent loops between SW1, SW2, SW3 and SW4, we need to configure the STP protocol:

- The STP mode is MSTP and the domain name is ***huawei***.
- VLAN 20 belongs to Instance 1, VLAN 30 belongs to Instance 2;
- In Instance 1, SW1 is the primary root bridge and SW2 is the backup root bridge. In Instance 2, SW2 is the primary root bridge and SW1 is the backup

root bridge.

3.5 OSPF

To implement Layer 3 interworking within the headquarters network, the IGP uses the OSPF routing protocol.

SW1 (VLANif10, VLANif 20, VLANif30, Loopback 0), SW2 (VLANif10, VLANif 20, VLANif30, Loopback 0), FW1 (GE1/0/0, GE1/0/1, Loopback 0), FW2 (GE1/0/0, GE1/0/1, Loopback 0) need to run OSPF protocol, the process ID is 1, and the area is 0.

3.6 Security Zone

Configure the security zone of the firewall. G1/0/1 of FW1 and FW2 must be added to the Trust zone. G1/0/0 interfaces must be added to the Untrust zone. G1/0/6 interfaces must be added to the DMZ zone.

3.7 Firewall Security Policy and Hot Standby

The firewall is deployed in active/standby mode. FW1 is the primary and FW2 is the standby. The firewall starts related security policies such as services and interconnection.

The VRRP/VGMP function is enabled on the G1/0/0 interface. The virtual IP address is 10.1.127.10. The G1/0/6 interface is an HRP heartbeat interface.

The routes between headquarters and branches are required to be reachable. The data traffic need to be released from the Trust zone to the Untrust zone (The policy name is trust_untrust). The date traffic from Untrust zone to Trust zone must be matched exactly (The policy name is untrust_trust).

3.8 BGP

To implement network interworking between the headquarters and branches, the BGP protocol is used.

The AS number of the headquarters is 100. FW1, FW2, SW1, and SW2 use the logical interface (Loopback 0) to establish the IBGP neighbor relationships.

The AS number of the branch is 200. R1 and the Firewall use the physical interface to establish the EBGP neighbor relationships.

Enable headquarters and branches to learn the routes from each other.

3.9 WLAN

3.9.1 DHCP

Configure Layer 3 interworking between APs, ACs, and neighboring network devices. All APs and wireless terminals obtain an IP address through DHCP. Use the global mode on the SW1 to configure DHCP services for APs and STAs. The global address pool names are ***ap*** and ***huawei***.

Table 3-3 WLAN DHCP allocation table

Project	Data
AP Management VLAN	VLAN15
STA Service VLAN	VLAN20
DHCP Server	SW1 acts as a DHCP server to assign an IP address to the AP. SW1 acts as a DHCP server to assign an IP address to the STA. The default gateway of the STA is 10.1.20.13.
IP address pool of the AP	10.1.15.0/24（Except 10.1.15.2）
IP address pool of the STA	10.1.20.0/24
Source IP address of the AC	8.8.8.8

3.9.2 AP on-line configuration

Configure the WLAN management VLAN. The ap-name is ***AP1*** and ap-group name is ***Huawei***.

Configure AP authentication mode as MAC address authentication.

3.9.3 Configuration and Delivery

Configure WLAN service parameters to implement STA access to the WLAN network. All template names are ***huawei***.

Configure the security policy of WPA2. The password is ***Huawei@123***. Encryption method is aes-tkip.

The SSID is ***huawei*** and the service forwarding mode is tunnel forwarding.

3.10 Verification

After all the configuration is completed, STA and PC will be able to automatically obtain the IP address, and all the terminal can communicate with each other.